ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Καραμπινάκης Εμμανουήλ
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
Επόπτης Μεταπτ. Εργασίας: Καθηγητής, Ε. Μαρκάτος

Τετάρτη, 27/11/2019, 10:00
Αίθουσα Β106, Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

" Ταυτοποίηση έξυπνων οικιακών συσκευών και αναγνώριση των εντολών τους από την διαδικτυακή κίνηση και ο ρόλος των εικονικών βοηθών"

ΠΕΡΙΛΗΨΗ

Οι έξυπνες οικιακές συσκευές είναι μεγάλο κομμάτι της καθημερινότητάς μας και τείνουν να γίνουν μια αναγκαιότητα στην ζωή μας που χαρακτηρίζεται από γρήγορους ρυθμούς. Οι συσκευές που απαρτίζουν το διαδίκτυο των πραγμάτων έχουν ομολογουμένως λύσει πολλά και διάφορα προβλήματα της καθημερινότητάς μας. Με την εισαγωγή των έξυπνων αυτών συσκευών στα σπίτια μας, η ασφάλεια και η προστασία της ιδιωτικότητας που απαιτείται από αυτές πρέπει να ληφθεί πιο σοβαρά υπόψιν, ιδίως όταν η φύση αυτών των συσκευών απαιτεί να αλληλοεπιδρούν ή να διαχειρίζονται ευαίσθητα και προσωπικά δεδομένα. Το Amazon Echo είναι ένα έξυπνο ηχείο το οποίο μπορεί να καταλάβει εντολές σε ανθρώπινη φυσική γλώσσα και να απαντήσει ή να εκτελέσει αιτήματα του χρήστη επικοινωνώντας με την Alexa, έναν εικονικό βοηθό που βρίσκεται σε διαδικτυακό σύννεφο, όπου οι εντολές αναλύονται και εκτελούνται. Ο χρήστης ενεργοποιεί τον εικονικό βοηθό χρησιμοποιώντας μία λέξη αφύπνισης και έπειτα αλληλοεπιδρά με αυτόν με φωνητικές εντολές. Η Alexa είναι επίσης ικανή να συνδεθεί με άλλες

περιφερειακές έξυπνες συσκευές που βρίσκονται στο ίδιο τοπικό δίκτυο με το Echo, δημιουργώντας έτσι ένα έξυπνο σπίτι διασυνδεδεμένων συσκευών κάτω από τον εγκέφαλο της Alexa.

Θα παρουσιάσουμε πώς ένας πάροχος υπηρεσιών διαδικτύου ή οποιοσδήποτε άλλος παθητικός παρατηρητής της διαδικτυακής κίνησης, με πρόσβαση στην κίνηση δικτύου ενός χρήστη, είναι ικανός να αναγνωρίσει τους τύπους των έξυπνων συσκευών σε ένα οικιακό δίκτυο, να συμπεράνει την κατάσταση στην οποία βρίσκονται και πώς η διασύνδεση των έξυπνων συσκευών με έναν εικονικό βοηθό όπως το Alexa της Amazon, με τον τρόπο που υλοποιείται σήμερα, μπορεί να βοηθήσει σε αυτή την ταυτοποίηση. Θα αναλύσουμε κατά πόσο είναι ασφαλής, σε επίπεδα προστασίας προσωπικών δεδομένων, η χρήση εικονικών βοηθών αλλά και διαφόρων τύπων έξυπνων συσκευών που μπορούν να διασυνδεθούν με έναν εικονικό βοηθό. Ακόμα, θα παρουσιάσουμε και θα ομαδοποιήσουμε τις έξυπνες συσκευές βάσει της ασφάλειας που παρέχουν. Θα μελετήσουμε αφενός πόσο ασφαλής μπορεί να είναι μια τέτοια συσκευή με τα τωρινά δεδομένα, αφετέρου πόσο μή-ασφαλής μπορεί να είναι μια πιο ευάλωτη συσκευή, φτάνοντας στο σημείο κάποιος κακόβουλος όχι μόνο να συμπεράνει ευαίσθητα προσωπικά δεδομένα για τον χρήστη, άλλα και να παρέμβει στην λειτουργία της συσκευής.

Manolis Karabinakis
M.Sc. Thesis

Computer Science Department
University of Crete
Master's Thesis Supervisor: Professor, E. Markatos

Wednesday, 27/11/2019, 10:00
Room B108, Computer Science Dept., University of Crete

“Smart Home Devices Activity Fingerprinting From Their Network Traffic And The Role Of Virtual Assistant Devices”

ABSTRACT

Smart home devices are tending to become a necessity in our fast-paced life, Internet of Things (IoT) devices have proved to solve many of our everyday life problems of any kind. With the

introduction of IoT devices in our homes, security and privacy must be taken more seriously, especially when the nature of those devices is to interact or handle sensitive and personal data. Amazon Echo is a smart speaker that can understand natural language voice commands and complete tasks for the user by communicating with Alexa, a cloud-based virtual assistant where the commands are analyzed and comprehended. The user activates the device with a \wake up" word, then he interacts with it with voice commands. Alexa is also capable of connecting with peripheral smart devices at the same WiFi network, thus creating a smart home with interconnected devices under the brain of Alexa.

We will demonstrate how an ISP or any other passive network observer with access to a users last-mile network traffic is capable of identifying the types of smart home devices even behind Network Address Translation (NAT). Figure out their state, and how the interconnection of the smart devices with a virtual assistant like Amazon Alexa, in the way that is implemented now, is giving away privacy- sensitive information. We will analyze the security of Amazon Echo and a few different types of smart home devices that are Alexa compatible, and we will describe the process of how a malicious network observer can infer information about the user. Also, we will present and cluster the security of IoT devices, how secure an IoT device can be with the existing implementation and on the other hand, how insecure is a more vulnerable smart device at the point where an attacker can not only extract sensitive information about the user's life but also actively interfere with its usage.